



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : G06F 1/00	A1	(11) International Publication Number: WO 00/54127 (43) International Publication Date: 14 September 2000 (14.09.00)
(21) International Application Number: PCT/US00/05986		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
(22) International Filing Date: 8 March 2000 (08.03.00)		
(30) Priority Data: 09/264,339 8 March 1999 (08.03.99) US		
(71) Applicant: SPYRUS, INC. [US/US]; 5303 Betsy Ross Drive, Santa Clara, CA 95054 (US).		
(72) Inventors: WILLIAM, P., Bialick; 7150 Moorland Drive, Clarksville, MD 21029-1735 (US). RUSSELL, D., Housley; 918 Spring Knoll Drive, Herndon, VA 20170 (US). CHARLES, R., J., Moore; 219 Buckland Road, Nundah, Brisbane, QLD 4012 (AU). DUANE, J., Linsenbardt; 5532 Sweigert Road, San Jose, CA 95132 (US).		
(74) Agent: GRAHAM, David, R.; 1337 Chewpon Avenue, Milpitas, CA 95035 (US).		
(54) Title: METHOD AND SYSTEM FOR ENFORCING ACCESS TO A COMPUTING RESOURCE USING A LICENSING CERTIFICATE		
(57) Abstract		
A licensing attribute certificate enables a trusted computing base to enforce access to a computing resource by a computer application. The licensing attribute certificate can contain enforcement data which limits the use of the computing resource. The licensing attribute certificate can also contain information allowing for the tracking of licensing data about the use of the computing resource. The use of a licensing attribute certificate to enforce access to a computing resource can allow products to be fielded which have their capability limited to a specific subset of functions. The enforcement data, the licensing data, and the data limiting the application to a specific subset of functions are cryptographically bound to the computing resource using a licensing attribute certificate according to the invention. Prior to allowing access to the computing resource by the computer application, a trusted computing base strongly authenticates that usage via the licensing attribute certificate.		<p>The diagram illustrates the architecture for enforcing access to a computing resource using a licensing certificate. It shows the interaction between a User, a Computer Application, an Executable Application, a SPEX™ Library, and a Cryptographic Token.</p> <ul style="list-style-type: none"> User: Interacts with the Computer Application. Computer Application: Manages the User interaction and interacts with the Executable Application and the SPEX™ Library. Executable Application: Interacts with the Computer Application. SPEX™ Library: Contains the LMS-CAPT (Licensing Management System-Cryptographic Token) and the Hardware Token Code Stack. <ul style="list-style-type: none"> LMS-CAPT: Manages the Licensing Attribute Certificate (LAC) and the License Management Key (LMK). Hardware Token Code Stack: Manages the Hardware Token Code Stack (HTCS). Cryptographic Token: Manages the Resource Manager and the Resource Manager Key (RMK). <ul style="list-style-type: none"> Resource Manager: Manages the Resource and the Resource Key (RK).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

METHOD AND SYSTEM FOR ENFORCING ACCESS TO A COMPUTING RESOURCE USING A LICENSING CERTIFICATE

5

10

BACKGROUND OF THE INVENTION**Field of the Invention**

The present invention relates generally to the authorized use of computing resources by computer applications. More particularly, the present invention relates to use of a licensing attribute certificate (LAC) to provide cryptographic binding between a computing resource and attributes related to a computer application, and to provide strong authentication by a trusted computing base controlling the computing resource.

25

Background Information

In a typical untrusted computer environment, a computer application can use available computing resources with little or no authorization or accountability. Examples of such computing resources include a modem or network interface. Another example of such computing resources includes a cryptographic token, which provides cryptographic resources to the computer application.

Fig. 1a depicts a typical computer system 100 made up of several "layers" 101, with two layers 130 and 132 consisting of a number of different modules 102, 103, 104,

and 105. Each layer represents a collection of one or more modules at a particular abstraction level in a hierarchy of software code development. Each module represents a collection of computer instructions which perform a particular operation on the data which the module receives, producing some data output from the module. At the top layer 130, module 102 can represent a computer application running on a computer of a user 115. Via a user interface in this example, module 102 receives input 110 from user 115. The input 110 could, for example, represent ordering and payment information in an electronic commerce transaction.

Similarly, module 103 receives data item 112, data item 114, and data item 116 as inputs. The module 103 processes the data items 112, 114, and 116, and produces data outputs 118 and 120. These outputs 118 and 120, in turn, become inputs for computing resource A 106. Computing resource A 106 then processes its data inputs 118, 120, 122, and 124 to produce resource output 126, which is returned to module 102.

In the example system shown in Fig. 1a, layer 130 might be written in a well known high-level language, such as C or C++. Layer 132 can comprise libraries of lower-level functions, that would be usable by other applications in addition to module 102. These libraries could also be written in a high-level language.

In general, layer 134 represents any atomic computing resources that process data. Layer 134 can be cryptographic computing resources, such as those found on a cryptographic token. Layer 134 can also be computing resources that send signals to hardware devices, such as a display or some other peripheral device. Layer 134 can

also be computing resources that transform data received from user 115.

A cryptographic token provides the ability to perform cryptographic operations on data. Some examples of 5 cryptographic operations include symmetric encryption (secret key) operations, asymmetric encryption (public key) operations, key exchange operations, hash operations, digital signature operations, and key wrapping operations.

Fig. 1b depicts an example of a system 150 of 10 functional layers that contain computing resources specifically designed for providing cryptographic processing. This system, which does not contain the invention, can be contrasted with the system shown in Fig. 4, which does contain the invention. In the example shown 15 in Fig. 1b, user 152 interacts with a user interface in the computer application 171 of application layer 160. In this example, computer application 171 represents the highest level of abstraction; that is, an interface with user 152. As a result of input 170 from user 152, computer 20 application 171 generates inputs 172 and 174 for a mid-level application programmer interface (API) layer 162. In this example, the mid-level API layer 162 comprises two different mid-level libraries, cryptographic API library A 173 and cryptographic API library B 175. These API 25 libraries 173 and 175 communicate with a low-level API library 177 in low-level API layer 164 via inputs 176 and 178. Finally, the low-level API library 177 communicates with the cryptographic resources via inputs 180 and 182 to software drivers comprising hardware token code stack 179 30 or software token code stack 181 in driver software level 166. Hardware token code stack 179 interfaces with hardware cryptographic token reader 183. Hardware cryptographic

token reader 183 sends data over data path 184 to hardware cryptographic token 187 in order for the data to be cryptographically processed therein. The hardware cryptographic token 187 contains trusted computing base 5 (TCB) 191 which is used to provide computing resources to computer application 171 in the form of cryptographic operations from cryptographic computing resource A 193. Another example of a TCB which can be used to provide cryptographic operations from cryptographic computing 10 resource B 197 to computer application 171 in system 150 is TCB 195 made accessible via software token 189. Software token 189, consisting, for example, of a floppy disk, is accessed via software token code stack 181 and token reader 185, and contains the necessary information to allow 15 computer application 171 to access the cryptographic operations made available via low-level API library 177.

Early cryptographic systems used a secret key approach to secure data. In these systems, each user had the same cryptographic key which was used for both encryption and 20 decryption of the data. As a result, the key needed to be kept secret or else the system could be compromised (thus the name secret key cryptography). In contrast, relatively recent advances in cryptography have led to cryptographic systems which use a mathematically related pair of keys. 25 In these systems, one key is kept private by the user, while the other is made public (thus the name public key cryptography). These key pairs allow for algorithms that provide confidentiality (via encryption); and authentication, integrity, and nonrepudiation (via digital 30 signatures).

The deployment of public key cryptography, especially in a public key infrastructure (PKI), relies heavily on

public key certificates. A public key certificate (or just "certificate") contains the public key of a user, along with information that allows a relying party to evaluate whether or not to trust a user's digital signature produced 5 using the private key corresponding to that public key. In particular, the certificate contains the digital signature of a Certification Authority (CA). In general, the CA is a secure, standards-based, and trusted entity that provides certificate, token, user registration, and directory 10 management services. In particular, the CA issues certificates to subscribers. A CA's signature on a certificate indicates that the CA has verified the identity of the user whose certificate it has signed, and the CA's signature also binds the identity of the user to the public 15 key appearing in the certificate.

The X.509 standard of the International Telecommunication Union (dated 6/97) defines an "attribute certificate" as a "set of attributes of a user together with some other information, rendered unforgeable by the 20 digital signature created using the private key of the certification authority which issued it." Thus, an attribute certificate contains information to supplement the identity information in a public key certificate.

In addition, the X.509 standard defines "strong 25 authentication" as "[a]uthentication by means of cryptographically derived credentials". The X.509 standard discusses the property of some public key cryptosystems (PKCSs) in which the enciphering and deciphering steps can be reversed, and goes on to state that this property 30 "allows a piece of information which could only have been originated by X, to be readable by any user (who has possession of [the public key of X]). This can, therefore,

be used in the certifying of the source of information, and is the basis for digital signatures. Only PKCS which have this (permutability) property are suitable for use in this authentication framework." In other words, strong
5 authentication can only be achieved with a PKCS in which the public key reverses the transformation accomplished using the private key, and vice versa.

The Trusted Computer System Evaluation Criteria from the United States Department of Defense (DOD) defines a TCB
10 as "the totality of protection mechanisms within a computer system...the combination of which is responsible for enforcing a security policy. It creates a basic protection environment and provides additional user services required for a trusted computer system." An appropriately designed
15 cryptographic token can, for example, contain a TCB. Appropriate design might include features such as a tamper proof case, nonmodifiable firmware, and zeroization of sensitive data upon intrusion detection. A secure operating system is another example of a TCB.

20 In the past, systems have been suggested which provide access control over various distributed computer resources. For example, in U.S. Pat. No. 5,339,403 issued to Parker, a system is described which requires a user to present a privilege attribute certificate to a computer application
25 in order to access that application. However, the system according to Parker assigns the privilege attribute certificate to the user, only providing access control over the user to some subset of target computer applications. The system according to Parker does not provide strong
30 authentication as the means for allowing access from a computer application to a computing resource. Furthermore, the system according to Parker utilizes a very complex

shared secret (i.e. secret key) approach. The Parker approach relies upon encryption of the privilege attribute certificate using the shared secret key. A secret key system contains inherent key management problems and key compromise problems. In particular, a purely secret key system has no recovery mechanism following a compromise. The only way to recover (i.e. the only way to again provide security after compromise of a secret key) is via a physical redistribution of secret key material.

In addition, prior systems have been developed which provide access control over portable data storage media in a manner which allows tracking the usage of certain data. For example, commonly owned U.S. Pat. No. 5,457,746 issued to Dolphin on October 10, 1995, describes a system which allows a publisher to define and enforce attributes related to encrypted files stored on external media. The attributes in this system could relate to such things as usage of particular data, time-related usage of a resource, or number of log-ons.

For many reasons, it is desirable to control the use of computing resources by a computer application through the use of strong authentication. For example, certain computing resources available on cryptographic tokens, if accessible by the computer application, would render the token unable to be exported from certain countries (such as the United States) unless restricted to use by approved computer applications. If those cryptographic operations could be successfully limited to use by approved computer applications using strong authentication, the cryptographic token could then be exported.

Similarly, it may be desirable to limit the accessibility to cryptographic operations contained in a

cryptographic token for licensing reasons, which would require a metering of those operations. For example, a provider of cryptographic products might desire to limit access to operations on a cryptographic token to those entities who have properly licensed those operations from the provider. Alternatively, it may be desirable for developers of software products to control accessibility to their products using strong authentication techniques provided by the use of an LAC, in conjunction with separate computing resources.

SUMMARY OF THE INVENTION

According to the invention, a licensing attribute certificate (LAC) enables strong authentication techniques to be utilized for enforcing access to computing resources, via the use of standards-based public key techniques. Enforcing can include, for example, controlling access to computing resources, metering usage of computing resources, selectively enabling certain functions available from computer resources, or any combination of these and other functions. The LAC can contain information allowing for the tracking of licensing data about the use of computing resources. Those computing resources can be contained within a trusted computing base (TCB). The TCB can be in any of a number of forms, including contained within a cryptographic token or a secure operating system. The LAC can further contain information which limits the use of the available computing resources. This would allow products to be fielded, such as cryptographic tokens which contain cryptographic computing resources, which have their capability limited to a specific subset of functions. The

use of a LAC in accordance with the invention can provide a cryptographically strong way of limiting access by a computer application to a specific subset of functions.

In one embodiment of the invention, a computer application developer receives a LAC from a vendor of a computing resource. A vendor can include any person or entity which provides computing resources. The developer embeds the LAC, containing a vendor's digital signature, into a computer application. The public key corresponding to the vendor's private key can be built in to the software library that provides the interface between the computer application and the TCB. Alternatively, the public key corresponding to the private key of the vendor can be built in to the TCB containing computing resources.

In yet another embodiment, separate public keys can be built in to both the software library and the TCB. When the computer application attempts to use a computing resource within the TCB, the library seeks to verify a first digital signature of the vendor and the TCB seeks to verify a second digital signature of the vendor. In addition to checking that both of the digital signatures are valid, checks could be made on the enforcement data within the licensing attribute certificate to determine whether access to the computing resources within the TCB can take place.

This invention provides a method for enforcing access by a computer application to a computing resource controlled by a trusted computing base, using standards-based public key techniques. The invention uses strong authentication to enforce that access control. The invention thus overcomes the complexities in the data exchanges involved in prior art systems. The invention

also provides strong authentication in the use of a computing resource by a computer application, and eliminates the security risks particularly associated with systems which implement secret key approaches. The 5 invention also provides a method for tracking usage of a computing resource using a LAC. Furthermore, the invention provides a method for allowing computer application developers to control access to their products via use of a LAC. In addition, the invention provides a method for 10 restricting the usage of a computing resource to authorized functions.

BRIEF DESCRIPTION OF THE DRAWINGS

15

Fig. 1a and Fig. 1b depict the arrangement of software modules in layers, including software layers that contain particular elements for providing cryptographic processing.

Fig. 2 depicts a basic architectural diagram showing a 20 licensing attribute certificate that has been installed in equipment belonging to a user.

Fig. 3a, Fig. 3b, and Fig. 3c depict a method, according to the invention, of using a licensing attribute certificate to cryptographically bind information about a 25 computer application and computing resources contained within a trusted computing base.

Fig. 4 depicts an example, according to the invention, of the cryptographic binding between a computer application and a trusted computing base which provides cryptographic 30 resources.

Fig. 5 depicts the contents of one embodiment of a LAC.

Fig. 6 depicts a process, according to the invention, of producing the token related information in the licensing attribute certificate.

Fig. 7 depicts a process, according to the invention, 5 of producing the library related information in the licensing attribute certificate.

Fig. 8 depicts a library enforcement process, according to the invention.

Fig. 9 depicts a token enforcement process, according 10 to the invention.

Fig. 10 depicts an example, according to the invention, of a token enforcement process which checks a counter to determine whether or not a certification authority can issue a certificate.

15 Fig. 11a and Fig. 11b depict two models of licensing attribute certificate implementation, according to the invention.

20 DETAILED DESCRIPTION OF THE INVENTION

According to the present invention, a method and system for cryptographically binding a computing resource and a licensing attribute certificate (LAC) allows only 25 authorized usage of the computing resource. The computing resource can, in one embodiment, be located within a trusted computing base (TCB). In another embodiment, the computing resource can be located outside of the TCB. In either case, the operations available from a computing 30 resource cannot be accessed without a cryptographic verification by the TCB of the computer application's use of that computing resource. In a further particular embodiment, a LAC is used to provide strong authentication

of a computing resource by a cryptographic token via a digital signature.

Fig. 2 depicts a basic system involving a LAC, according to the invention. User equipment 205 contains 5 TCB 208, computer application 210, and LAC 220. User equipment 205 can include any type of computational device. Some examples include a personal computer, a personal digital assistant, or a machine with embedded computing capability. In general, user equipment represents any 10 equipment used by a person or other entity (such as a corporation) that contains at least one computer application and at least one computing resource.

LAC 220 in Fig. 2 contains attribute information about computing resource 226, in the form of enforcement data 15 222. Enforcement data 222 facilitates enforcement of the use of the computing resource and can contain, for example, information about how and when the computing resource can be used. Enforcement data 222 can further contain information about what operations available from the 20 computing resource can be used. LAC 220 also includes digital signature 224 computed using a private key.

TCB 208 in Fig. 2 contains computing resource 226, to which TCB 208 controls access, as represented by the switch in data path 230. TCB 208 also contains a public key 212, 25 corresponding to the private key that was used to compute digital signature 224. Prior to computer application 210 gaining access to computing resource 226, TCB 208 must authenticate LAC 220 using public key 212. If the authentication of LAC 220 succeeds, TCB 208 will permit 30 computer application 210 to access computing resource 226 along data path 230.

Fig. 3a depicts a method according to the present invention as applied to enforcement of authorized usage (e.g. licensing) of computing resources. Other applications of the invention can include, for example, 5 exportability compliance or allowing selective usage of a computing resource.

In Fig. 3a, vendor 301 of a computing resource 360 (shown in Fig. 3c) first produces enforcement data 312 that can, for example, correspond to particular rights afforded 10 to a specific computer application developer 303 (shown in Fig. 3b). For example, the vendor of a computing resource might wish to limit the access to that computing resource to only a certain application. Alternatively, the vendor of the computing resource might wish to grant access to a 15 subset of all of the functionality available from the computing resource. For example, where the computing resource is a hardware cryptographic token, the vendor might wish to only allow digital signature operations to be executed and would therefore need to disallow encryption 20 operations.

In Fig. 3a, vendor 301 uses its private key 310 to compute digital signature 316 on enforcement data 312 using sign process 314. Sign process 314 (as well as other sign processes discussed herein) can be implemented using any of 25 the well understood techniques for computing a digital signature. For example, the Digital Signature Algorithm, as specified in Federal Information Processing Standard Publication (FIPS PUB) 186 could be used to calculate digital signature 316. Alternatively, the RSA algorithm 30 could be used.

Digital signature 316, corresponding to the particular computing resource 360, is combined with enforcement data

312 to form LAC 318. Vendor 301 then transmits LAC 318 to computer application developer 303. The transmission of LAC 318 to computer application developer 303 can occur using any methods and apparatus, including both networked and non-networked approaches. The LAC could be sent via a network, such as, for example, a Local Area Network (LAN), a Wide Area Network (WAN), or via the Internet. Transmission methods can include such things as, for example, electronic mail from the vendor to the computer application developer. Alternatively, the LAC can be posted on a bulletin board system (BBS), or can be stored in a directory of a computer system by the vendor and retrieved by the application developer using any type of retrieval technique, such as, for example, Telnet.

In Fig. 3b, computer application developer 303 generates computer application source code 330, which is combined with LAC 318. Computer application source code 330 and LAC 318 can be combined by using compile process 332, which creates an association between the computer application source code 330 and LAC 318. In another embodiment, a computer application and a LAC can be combined by providing an entry in a system registry of a computer operating system.

In Fig. 3b, the compilation of computer application source code 330 and LAC 318 generates an executable application 334 which can contain computer application 333 with LAC 318 embedded within it. Once compiled, the executable application 334 can be made available for distribution to users.

In Fig. 3c, user 305 can acquire the executable application 334 (which, in this example, contains the version of computer application 333 that can be executed on

a computer) through any of several means including, for example, retail store purchase, electronic purchase (e.g., via the Internet), or any other software distribution mechanism. User 305 can make a purchase of, for example, a 5 CD-ROM containing executable application 334, or can purchase and then download executable application 334 electronically. User 305 loads executable application 334 onto the user's computer 340 and runs executable application 334. In this example, executable application 334 10 needs to utilize computing resource 360 contained within TCB 345 (which can be contained within computer 340).

However, in order to gain access to computing resource 360, digital signature 316 contained within LAC 318 must be 15 verified by TCB 345. TCB 345 performs verify process 370 using public key 354 in combination with enforcement data 312 to verify digital signature 316. The success of verify process 370 means that digital signature 316 in LAC 318 is valid. In addition, supplemental enforcement data 356, 20 which may be contained in a database within computer 340 (i.e. external from the LAC), could be utilized to provide further control over accessibility to computing resource 360 as further described with reference to Fig. 10. Once LAC 318 is validated, executable application 334 being used 25 by user 305 will then have access to computing resource 360.

In order to verify digital signature 316, TCB 345 must have public key 354. In one embodiment, depicted in Fig. 3c, vendor 301 can embed public key 354 in TCB 345. In an 30 alternative embodiment, TCB 345 can receive public key 354 via a separate X.509 identity certificate path which is transmitted along with LAC 318.

Fig. 4 depicts a system 400 according to one embodiment of the invention which includes computing resources specifically designed for providing cryptographic processing. This embodiment represents one aspect of the 5 SPYRUS S2CA, made and sold by SPYRUS, Inc. of Santa Clara, California, which is a secure, standards-based, and trusted certification authority (CA) that provides certificate, token, user registration, and directory management services.

10 In system 400 in Fig. 4, user 480 installs and runs executable application 411 on the user's computer. Executable application 411 can contain a number of different types of computer functionality, including such things as user interfaces, software libraries, and device 15 drivers. In this example, the executable application 411 can contain LAC 403 which can be embedded in computer application 402. Also included in executable application 411 can be executable libraries, including PKCS #11 application programmer interface (API) 404 and Microsoft 20 CryptoAPI (CAPI) 406. PKCS #11 is a nonproprietary, technology-neutral programming interface for cryptographic tokens such as smart cards and PCMCIA cards. CAPI is an interface that allows developers to build applications that use system-level certificate management and cryptography.

25 Computer application 402 communicates with PKCS #11 API 404 via data path 412 and with CAPI 406 via data path 414. Upon execution of particular instructions in either PKCS #11 API 404 or CAPI 406 which require functionality contained within cryptographic computing resource 484, LAC 30 403 can be passed via either data path 416 or data path 418 to the vendor specific library, such as the SPYRUS Extensions (SPEX) library 408.

In Fig. 4, SPEX library 408 performs library authorization 800 which can include using library public key 410, library supplemental enforcement data 417, and LAC 403 in verify and validate process 415. Further detail on 5 library authorization 800 can be found in Fig. 8. The library authorization step provides an interim level of enforcement that does not involve a cryptographic token at all. This can be useful, for example, for minimizing the number of operations to be performed by the computing 10 resources. As long as verify and validate process 415 succeeds, SPEX library 408 will be permitted to communicate with hardware token code stack 430, in attempting to make use of cryptographic computing resource 484. In this example, cryptographic token 470 contains cryptographic 15 computing resource 484 which SPEX library 408 accesses via hardware token code stack 430 and smart card reader 460.

In this embodiment, control of the use of the cryptographic operations within the cryptographic computing resource 484 occurs within the boundaries of TCB 474 which 20 is contained within cryptographic token 470. These cryptographic operations can be carried out on a cryptographic token. For example, a LYNKS PCMCIA card or a Rosetta smart card, both made and sold by SPYRUS, Inc. of Santa Clara, California, provides all of the above 25 mentioned cryptographic operations to a computer application. Other examples of a hardware cryptographic token include a separate hardware board inside of a computer or an external hardware peripheral device. Alternatively, these cryptographic operations can be 30 carried out via the use of a software cryptographic token, which can comprise a computer processor executing instructions and accessing data stored on a data storage

device such as a floppy disk. For example, the software version of the Fortezza™ cryptographic token, also made and sold by SPYRUS, Inc. of Santa Clara, California, provides all of the above mentioned cryptographic operations to a computer application.

Prior to allowing any use of the cryptographic operations available in the cryptographic computing resource, TCB 474 performs token authorization 900 (described further below with respect to Fig. 9) which includes using token public key 490, token supplemental enforcement data 477, and LAC 403 in verify and validate process 482. The success of verify and validate process 482 confirms the cryptographic binding between cryptographic computing resource 484 and LAC 403. This allows TCB 474 to enforce the proper use of the cryptographic operations contained in cryptographic computing resource 484 by computer application 402.

The enforcement of the proper use of the cryptographic operations contained in cryptographic computing resource 484 can occur via the enforcement data contained in LAC 403. Enforcement data permits enforcement of various conditions represented by the data. Enforcement data can, for example, be defined such that computing resources are only available for a specified number of uses, or such that only certain functions within the computing resources are available. The bit pattern in the LAC in Fig. 5 represents one embodiment of the data used to provide enforcement. In another embodiment, a LAC can be implemented using the X.509 attribute certificate format.

LAC 403 in Fig. 5 contains enforcement data 520 which can include attribute data associated with both cryptographic token 470 and SPEX library 408. Token

attribute data 502 can, for example, identify the cryptographic operations on token 470 which are available to computer application 402 via SPEX library 408. Token digital signature 504 can be used by token 470 to validate 5 token attribute data 502 and to enforce the proper use of the cryptographic operations by computer application 402. Library attribute data 506 can represent the functionality available to computer application 402 via SPEX library 408. Library attribute data 506 can be further logically divided 10 into accessible tokens data 508 and sub-functionality data 510. These can allow even finer granularity to be defined for the subset of functions identified by library attribute data 506. For example, sub-functionality data 510 can be used in enforcing the available SPEX library functions such 15 as, for example, limiting the functions available to computer application 402 to only encryption and decryption, but not authentication.

In addition to the attribute data, LAC 403 in Fig. 5 contains library digital signature 514. Library digital 20 signature 514 can allow the SPEX library 408 to validate the LAC, and thereby control the availability of the library's functions.

Fig. 6 depicts a first step in the assembly of LAC 403 according to an embodiment of the invention. First, the 25 computing resource vendor generates token attribute data 502 associated with the particular computer application for which the LAC is being created. Once token attribute data 502 has been determined, the vendor uses token private key 602 to digitally sign token attribute data 502 using sign 30 process 604 which produces token digital signature 504.

Next, the vendor specifies information that determines the accessibility to the functions on the token. In the

LAC 403, accessible tokens data 508 represents this information. The vendor of cryptographic tokens can define, for example, accessible tokens data 508 such that access to the computing resources would be limited to only 5 those resources on that vendor's cryptographic tokens. After accessible tokens data 508 has been generated, the vendor then sets sub-functionality data 510 which can allow even finer granularity enforcement of the available resources. Once assembled, token attribute data 502, token 10 digital signature 504, accessible tokens data 508, and sub-functionality data 510 comprise enforcement data 520.

Fig. 7 depicts a subsequent step in the assembly of LAC 403 in the present embodiment. Once all of the enforcement data 520 associated with the token and the 15 library has been generated for LAC 403, the vendor uses a library private key 702 to digitally sign enforcement data 520 using sign process 704. The result is library digital signature 514, which is then appended to enforcement data 520. The overall data assembly, consisting of token 20 attribute data 502, token digital signature 504, accessible tokens data 508, sub-functionality data 510, and library digital signature 514 comprise LAC 403.

It may be desirable to use two different key pairs (each consisting of a public and a private key) for the two 25 signing processes 604 and 704 in Fig. 6 and Fig. 7, respectively. This means that token private key 602 in Fig. 6 and library private key 702 in Fig. 7 are different. This may be the case, for example, if the vendor of the token differs from the vendor of the library. 30 Alternatively, the two key pairs (and thus the two private keys 602 and 702) can be the same. This may be the case,

for example, if one vendor distributes both the token and the library.

Fig. 8 illustrates library authorization process 800 performed by SPEX library 408, as discussed generally in regards to verify and validate process 415 shown in Fig. 4. Upon receiving LAC 403, SPEX library 408 separates library digital signature 514 from the remainder of LAC 403. The enforcement data 520 is input to verify process 840, along with library digital signature 514 and library public key 410. If the library digital signature 514 is properly verified, the library 408 permits processing to continue. If the library digital signature 514 is not properly verified, SPEX library 408 notifies computer application 402 that an error has occurred. If an error does occur, the library can take a variety of courses of action such as using an alternate resource.

Once library digital signature 514 has been verified, the library 408 checks library attribute data 506 against library supplemental enforcement data 417. This can, for example, determine whether the library 408 is permitted to access the token or tokens designated in the accessible tokens data 508 and determine whether library 408 can perform the particular operations designated in sub-functionality data 510. If the validation of either accessible tokens data 508 or sub-functionality data 510 fails, data path 860 will not be enabled, which will prohibit the library 408 from further communications with the cryptographic token 470.

Fig. 9 illustrates token authorization 900 performed by token 410, as discussed generally in regards to verify and validate process 482 in Fig. 4. The token 470 separates the token digital signature 504 from LAC 403.

Token attribute data 502 is input to verify process 940, along with token digital signature 504 and token public key 480. If the token digital signature 504 is properly verified, the token 470 permits processing to continue. If 5 the token digital signature 504 is not properly verified, the token 470 notifies library 408 that an error has occurred. Library 408 then notifies computer application 402 of the error, and computer application 402 will handle the error. Computer application can notify user 480 of the 10 error, or can attempt to process the error without notifying user 480.

Once token digital signature 504 has been verified, token 470 checks token attribute data 502 against token supplemental enforcement data 477 in validate process 950. 15 This determines whether token 470 is permitted to perform the particular operations designated in token attribute data 502. If the validation fails, data path 960 is not enabled, which will prohibit the use of token 470 by computer application 402.

20 Fig. 10 depicts LAC 1000, according to an embodiment of the invention, which can be used for tracking usage of a particular computing resource. In this embodiment, the LAC 1000 exists in a system at a certification authority (CA) which issues certificates. In Fig. 10, token attribute 25 data 1070 contained in the LAC can contain usage data for a computing resource. This usage data allows the usage of the computing resource to be metered. For example, token attribute data 1070 in Fig. 10 contains a maximum certificates to issue field 1072. Token supplemental enforcement data 1074, which resides in a database that can 30 be maintained outside of a TCB, contains certificates issued counter 1076. Certificates issued counter 1076

reflects the number of certificates that have been issued by the CA. During validate process 1050, maximum certificates to issue field 1072 is compared against certificates issued counter 1076. If certificates issued 5 counter 1076 has exceeded the value in maximum certificates to issue field 1072, further usage of the computing resource will be disallowed.

The check of certificates issued counter 1076 against maximum certificates to issue field 1072 can occur inside 10 of the TCB. Once checked, the TCB would then update certificates issued counter 1076, store the updated value within the TCB, and send the updated certificates issued counter 1076 back to the database. In an alternative embodiment, the updating of the certificates issued counter 15 1076 can occur external from the TCB.

In another embodiment, the usage data can, for example, correspond to a maximum number of accesses by a computer application to a computing resource. In yet another embodiment, the usage data can, for example, 20 correspond to a maximum number of cryptographic operations that can be performed by computing resource which provide cryptographic functionality.

The embodiments of the LAC described so far represent only a few of many possible models of LAC usage. As the 25 model in Fig. 11a shows, vendor 1101 can distribute LAC 1102 (comprising enforcement data 1104 and digital signature 1106) to application developer 1108. Application developer 1108 creates computer application 1112 into which LAC 1102 is embedded, as previously described. Vendor 1101 30 also distributes computing resource 1115 and vendor public key 1119 (both contained within TCB 1110) to the user, who installs the TCB 1110 in user equipment 1114. The user

also installs computer application 1112, containing LAC 1102, in user equipment 1114. Prior to being able to use computing resource 1115, however, TCB 1110 would need to properly validate LAC 1102 using vendor public key 1119
5 contained in TCB 1110.

Fig. 11b shows a model which differs somewhat from that shown in Fig. 11a. In Fig. 11b, application developer 1120 creates computer application 1122 and has no interaction at all with vendor 1101. In contrast to the 10 model in Fig. 11a, the user sends request 1124 from user equipment 1114 to vendor 1101. In response, vendor 1101 prepares LAC 1103 and transmits this directly to the user. The user installs both LAC 1103 and TCB 1110 on user equipment 1114, in addition to computer application 1122.
15 In this model, similar to the model shown in Fig. 11a, prior to being able to use computing resource 1123, TCB 1110 must properly validate LAC 1103 using vendor public key 1121.

Although the invention has been described for a 20 licensing attribute certificate used by a CA, it applies to a wide range of computing applications where enforcing authorized usage of resources is desired. For example, usage of computer aided drawing (CAD) software could be enforced with a LAC. In addition, access to a CD-ROM 25 containing data could be enforced with a LAC. Thus, the present invention is not limited to the precise embodiments described above. For example, while a LAC could be compiled with a computer application as described above, a system and method according to the invention could just as 30 easily be implemented in which a LAC exists in a separate file from an executable application. Similarly, other authentication means besides digital signatures could be

used. Additionally, the counter discussed in the method for using a LAC to track usage of a resource might be contained within the cryptographic token itself.

It is clear that various changes and modifications may
5 be made to the embodiments which have been described, more
specifically by substituting equivalent technical means,
without departing from the spirit and scope of the
invention. The embodiments presented are illustrative.
They are not intended to limit the invention to the
10 specific embodiments described and shown in the attached
figures. Instead, the invention is defined by the
following claims.

CLAIMS

We claim:

5 1. A method for enforcing access by a computer application to a computing resource controlled by a trusted computing base, comprising the steps of:

generating enforcement data identifying usage of said computing resource;

10 embedding said enforcement data in a licensing attribute certificate;

 cryptographically binding said licensing attribute certificate to said computing resource using a private key;

15 associating said licensing attribute certificate with said computer application; and

 authenticating in said trusted computing base the use of said computing resource by said computer application using a public key corresponding to said 20 private key.

2. A method as in claim 1 wherein said generating step further comprises generating enforcement data in response to a request message for a licensing attribute 25 certificate received from a user.

3. A method as in claim 2 wherein said generating step is performed by a vendor.

30 4. A method as in claim 1 wherein said generating step further comprises generating library attribute data.

5. A method as in claim 4 wherein said generating step further comprises generating token attribute data.

6. A method as in claim 5 wherein said library attribute data further comprises accessible tokens data and sub-functionality data.

7. A method as in claim 6 wherein said generating step further comprises generating enforcement data corresponding to a particular set of access rights, comprising the steps of:

determining appropriate content of token attribute data; and

15 determining appropriate content of library attribute data.

8. A method as in claim 7 wherein said binding step further comprises:

20 computing a second digital signature on said token attribute data; and

including said second digital signature in said licensing attribute data.

25 9. A method as in claim 8 wherein the same private key is used to compute said second digital signature as that used to compute said first digital signature.

30 10. A method as in claim 9 wherein said private key used to compute said first and second digital signatures is a private key of a vendor of a library.

11. A method as in claim 8 wherein a different private key is used to compute said second digital signature from that used to compute said first digital signature.

5

12. A method as in claim 11 wherein said private key used to compute said second digital signature is the private key of a vendor of said computing resource.

10 13. A method as in claim 1 wherein said binding step further comprises computing a digital signature on said enforcement data.

14. A method as in claim 1 wherein said binding step 15 further comprises encrypting said enforcement data with a private key.

15. A method as in claim 1 wherein said associating step further comprises compiling computer application 20 source code with said licensing attribute certificate.

16. A method as in claim 1 wherein said associating step further comprises providing an entry identifying said licensing attribute certificate in a system registry of a 25 computer operating system.

17. A method as in claim 1 wherein said trusted computing base comprises a computer operating system.

30 18. A method as in claim 1 wherein said trusted computing base comprises a cryptographic token.

19. A method as in claim 18 wherein said binding step further comprises computing a digital signature on said enforcement data.

5 20. A method as in claim 1 wherein said licensing attribute certificate comprises an attribute certificate in X.509 attribute certificate format.

10 21. A method as in claim 1 wherein said authenticating step further comprises authenticating with a public key received in X.509 identity certificate format.

15 22. A method for allowing a trusted computing base to use a licensing attribute certificate to track usage of a computing resource by a computer application, comprising the steps of:

generating usage data;
embedding said usage data in said licensing attribute certificate;

20 cryptographically binding said licensing attribute certificate to said computing resource using a private key;

associating said licensing attribute certificate with said computer application;

25 updating a usage database within said trusted computing base in accordance with the usage of said computing resource;

authenticating in said trusted computing base the use of said computing resource by said computer application;

validating said usage database against said usage data for permitted usage of said computing resource; and

disallowing usage of said computing resource
5 if said validating step fails.

23. A method as in claim 22, wherein said usage data further comprises a maximum number of accesses by said computer application to said computing resource.

10

24. A method as in claim 22, wherein said usage data further comprises a maximum number of cryptographic operations to be performed by said computing resource.

15

25. A method as in claim 24 wherein said trusted computing base comprises a cryptographic token.

26. A method as in claim 25, wherein said cryptographic token comprises a PCMCIA card.

20

27. A method as in claim 25, wherein said cryptographic token comprises a smart card.

28. A system for enforcing access by a computer application to a computing resource controlled by a trusted computing base, comprising:
25

means for generating enforcement data;
means for embedding said enforcement data in a licensing attribute certificate;

30 means for cryptographically binding said licensing attribute certificate to said computing resource using a private key;

means for associating said licensing attribute certificate with said computer application; and a trusted computing base for authenticating the use of said computing resource by a computer application using a public key corresponding to said private key.

5 29. A system as in claim 28, wherein said computing resource comprises a cryptographic operation on a 10 cryptographic token.

30. A system as in claim 29 wherein said cryptographic token comprises a PCMCIA card.

15 31. A system as in claim 29 wherein said cryptographic token comprises a smart card.

32. A system as in claim 28 wherein said trusted computing base comprises a PCMCIA card.

20 33. A system as in claim 28 wherein said trusted computing base comprises a smart card.

34. A method for creating a licensing attribute 25 certificate for enforcing access by a computer application to a computing resource controlled by a trusted computing base, comprising the steps of:

generating enforcement data identifying usage of said computing resource;

30 embedding said enforcement data in said licensing attribute certificate;

cryptographically binding said licensing attribute certificate to said computing resource using a private key; and

5 associating said licensing attribute certificate with said computer application.

35. A method as in claim 34 wherein said generating step further comprises generating enforcement data in response to a request message for a licensing attribute
10 certificate received from a user.

36. A method as in claim 35 wherein said generating step is performed by a vendor.

15 37. A method as in claim 34 wherein said generating step further comprises generating library attribute data.

38. A method as in claim 37 wherein said generating step further comprises generating token attribute data.
20

39. A method as in claim 38 wherein said library attribute data further comprises accessible tokens data and sub-functionality data.

25 40. A method as in claim 39 wherein said generating step further comprises generating enforcement data corresponding to a particular set of access rights, comprising the steps of:

determining appropriate content of token
30 attribute data; and

determining appropriate content of library attribute data.

41. A system for creating a licensing attribute certificate for enforcing access by a computer application to a computing resource controlled by a trusted computing base, comprising:

means for generating enforcement data identifying usage of said computing resource;

means for embedding said enforcement data in said licensing attribute certificate;

means for cryptographically binding said licensing attribute certificate to said computing resource using a private key; and

means for associating said licensing attribute certificate with said computer application.

15

42. A system as in claim 41 wherein said means for generating said enforcement data further comprises means for responding to a request message for a licensing attribute certificate received from a user.

20

43. A system as in claim 42 wherein a vendor operates said means for generating said enforcement data.

44. A system as in claim 41 wherein said means for generating said enforcement data further comprises means for generating library attribute data.

45. A method as in claim 44 wherein said means for generating said enforcement data further comprises means for generating token attribute data.

46. A system as in claim 45 wherein said means for generating library attribute data further comprises means for generating accessible tokens data and sub-functionality data.

5

47. A system as in claim 46 wherein said means for generating said enforcement data further comprises means for generating enforcement data corresponding to a particular set of access rights, comprising:

10

means for determining appropriate content of token attribute data; and

means for determining appropriate content of library attribute data.

15

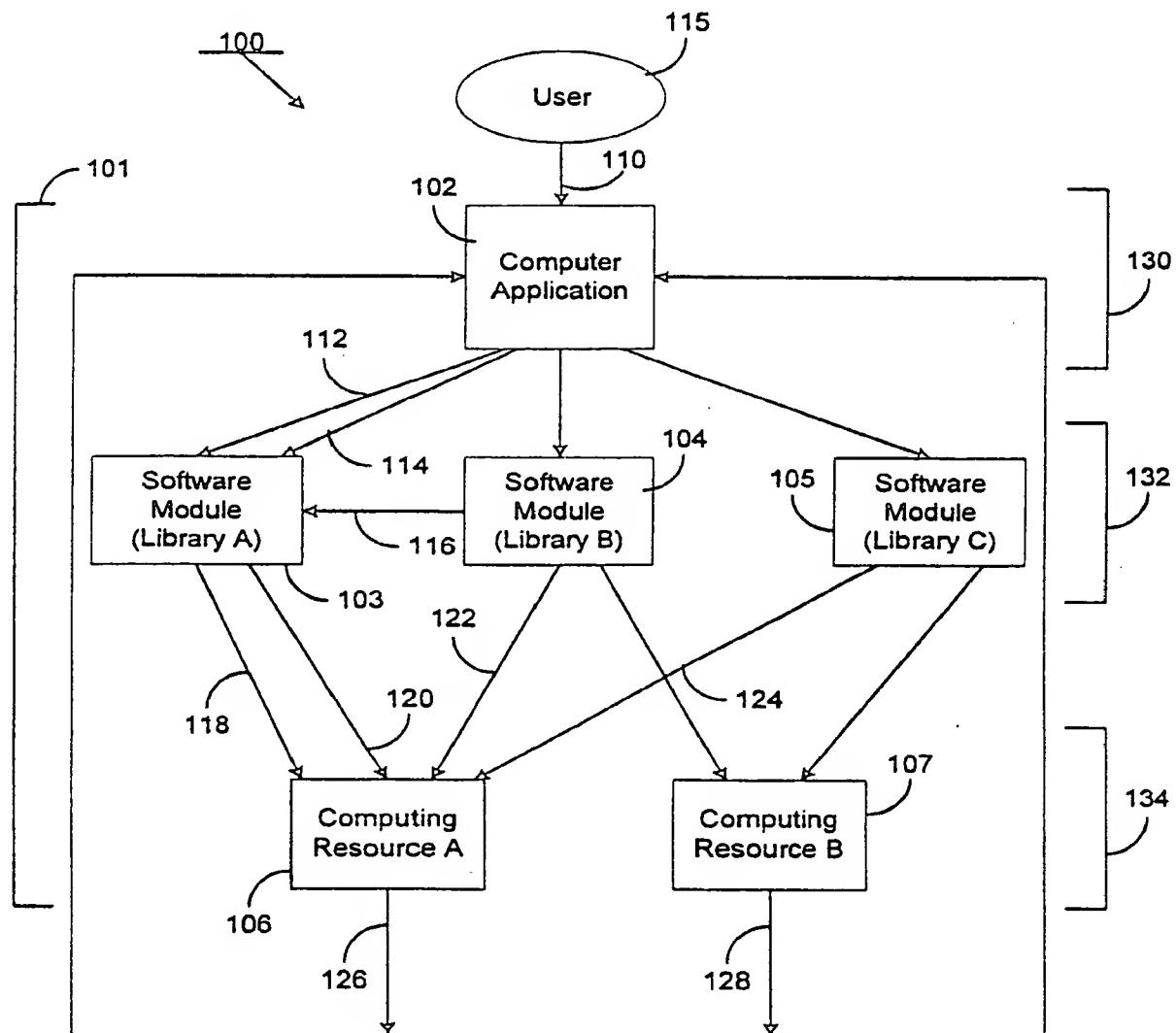


Fig. 1a

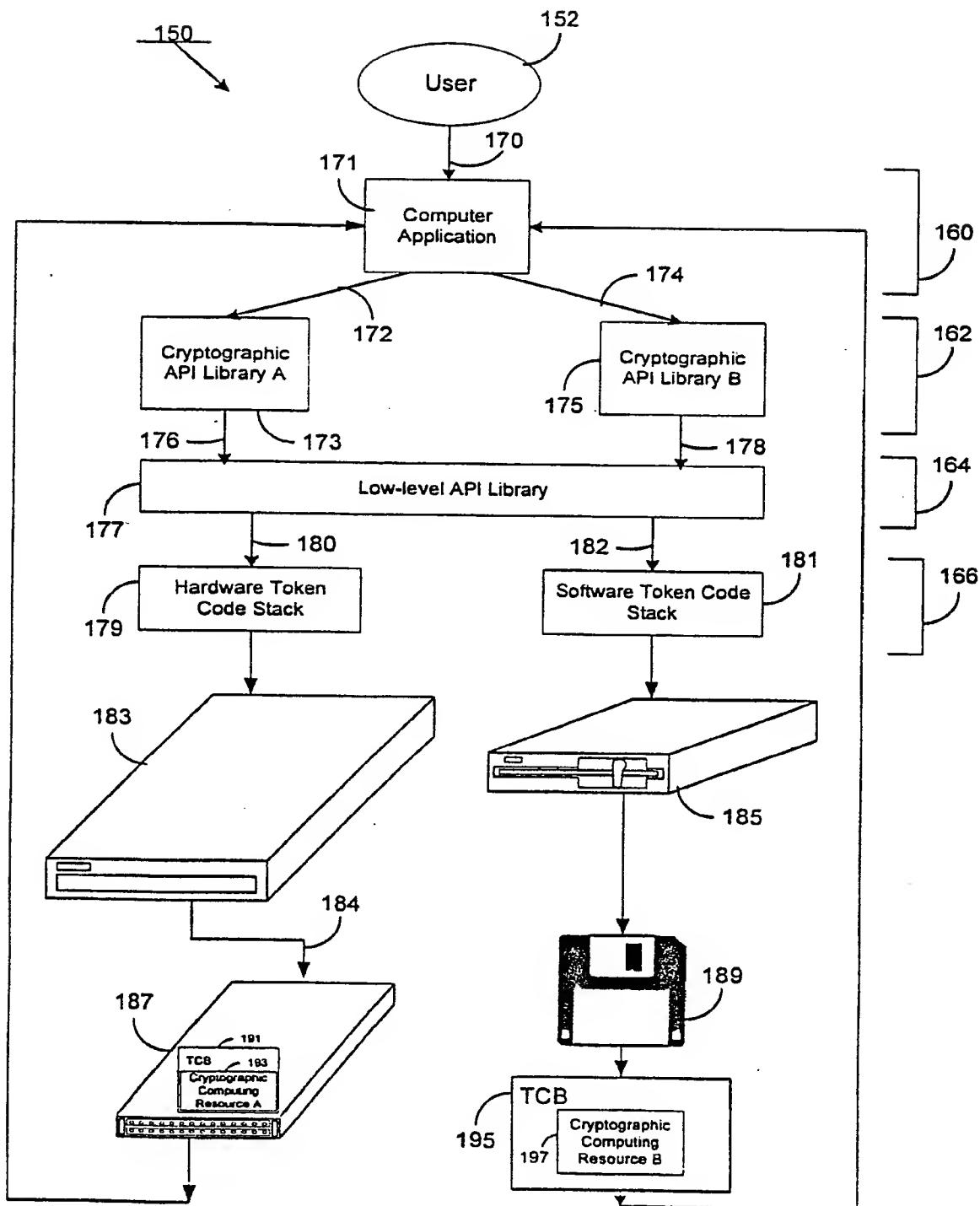


Fig. 1b

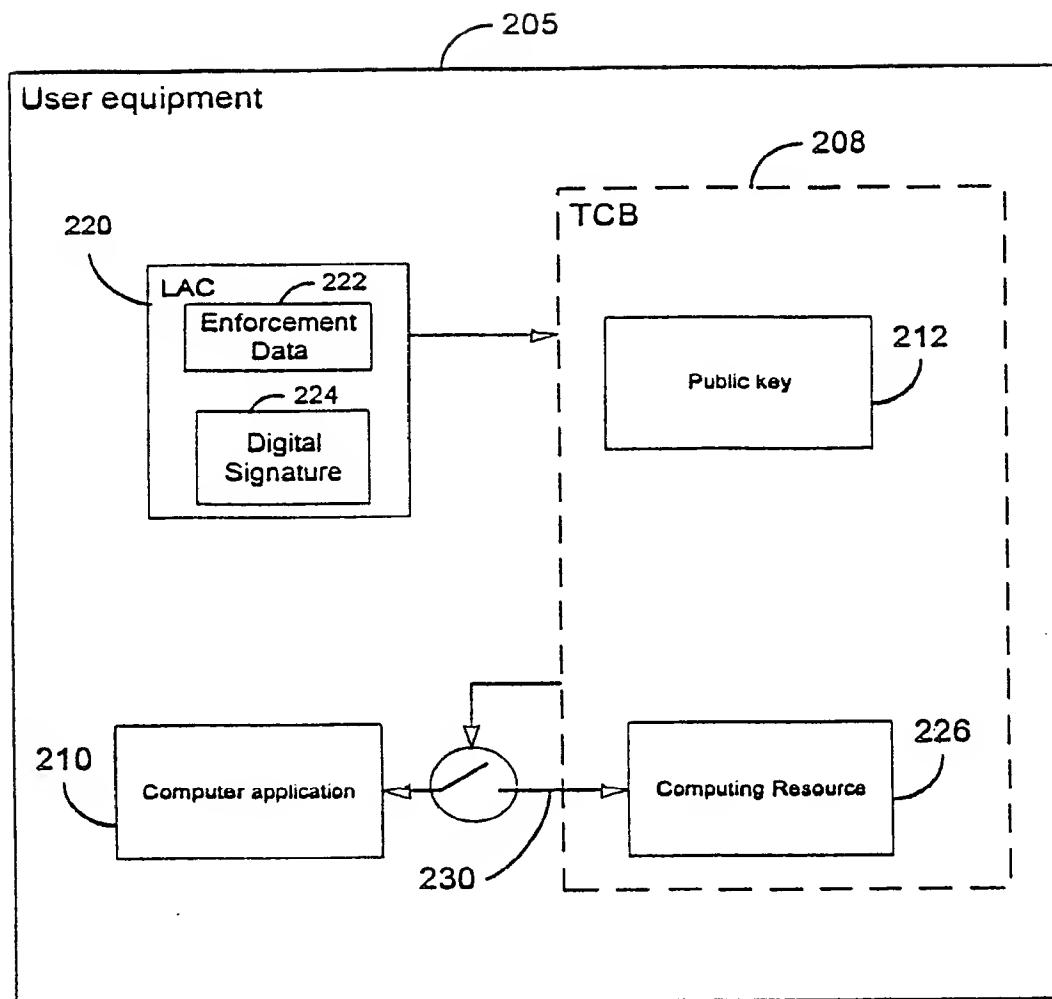


Fig. 2

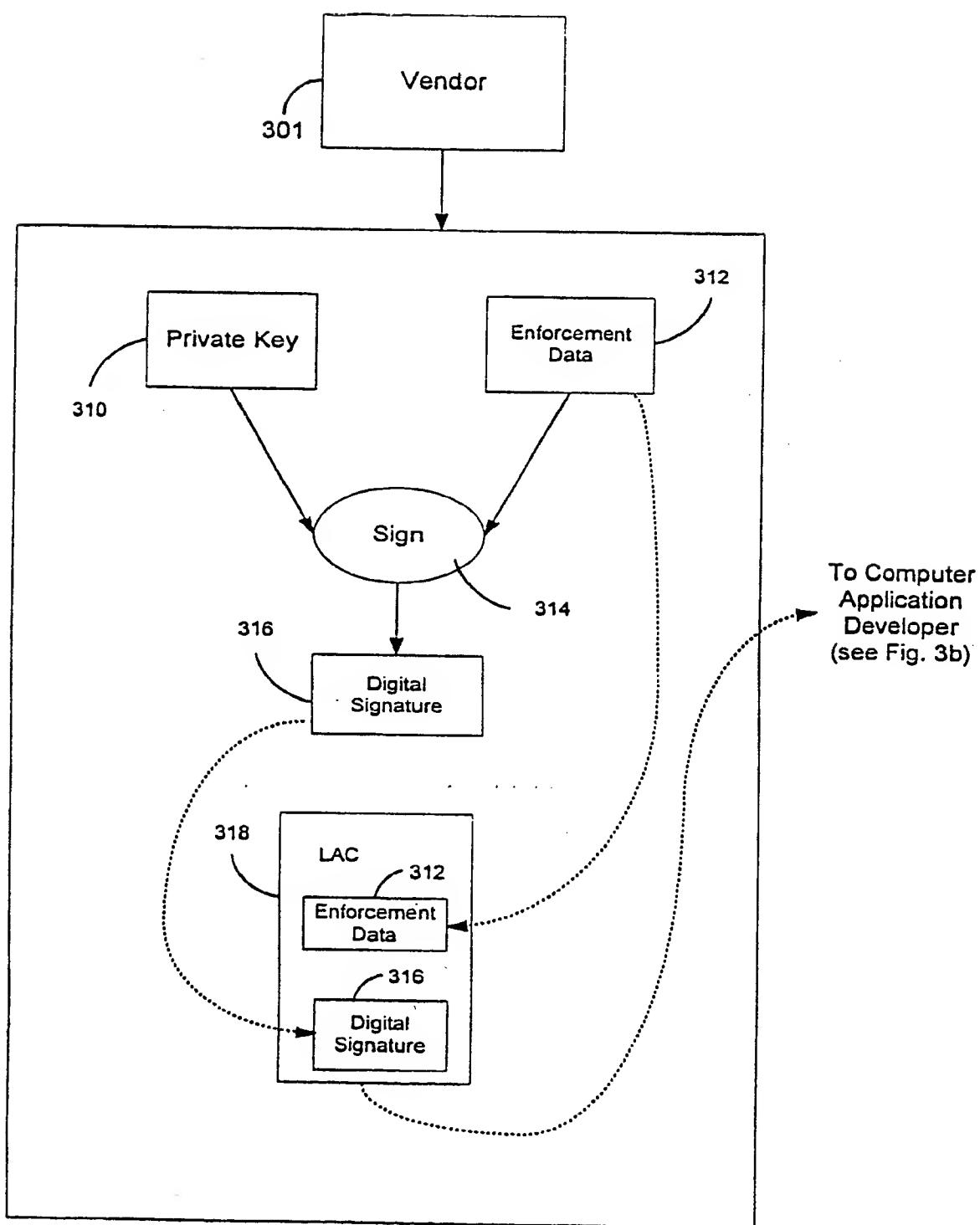


Fig. 3a

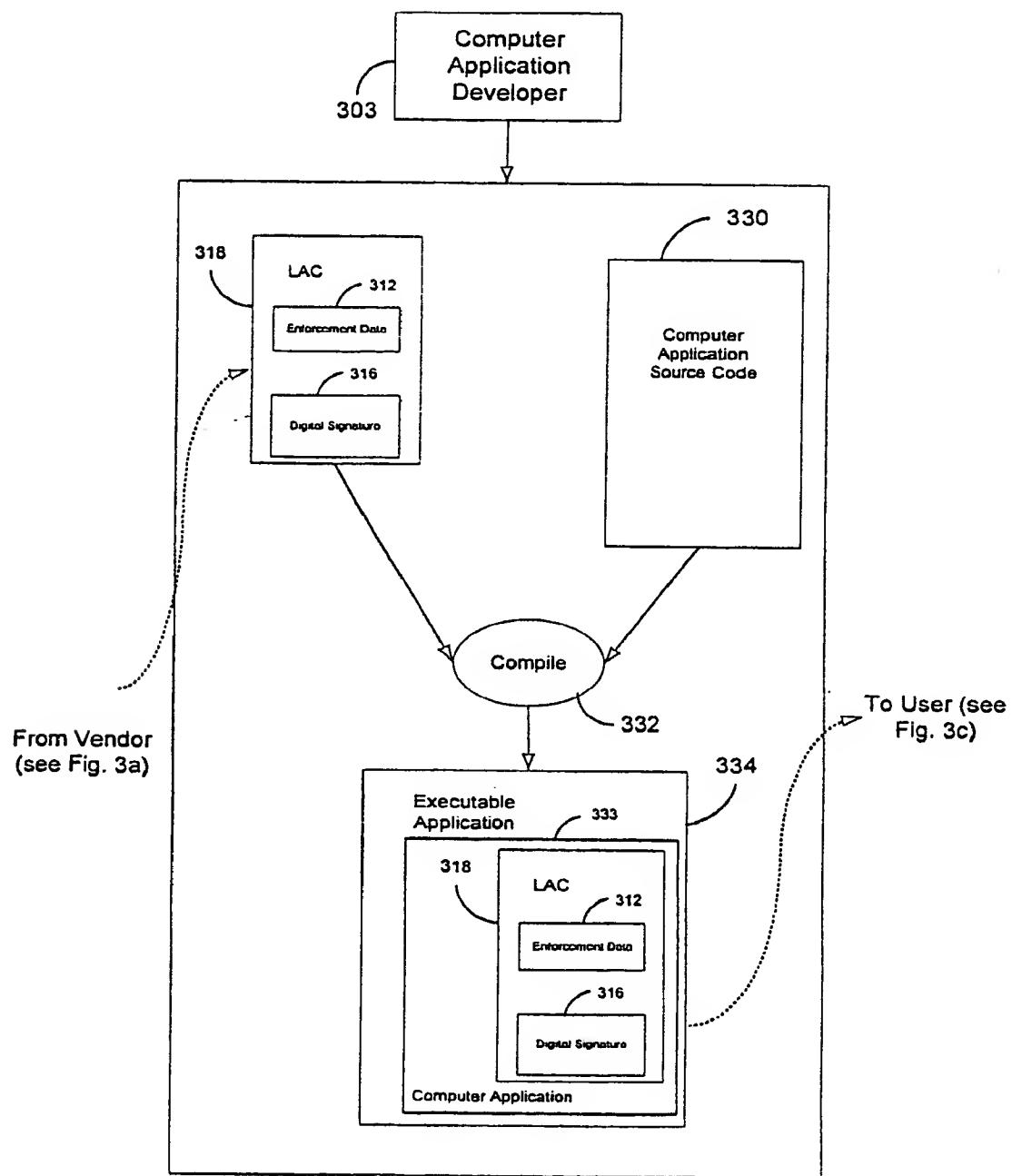


Fig. 3b

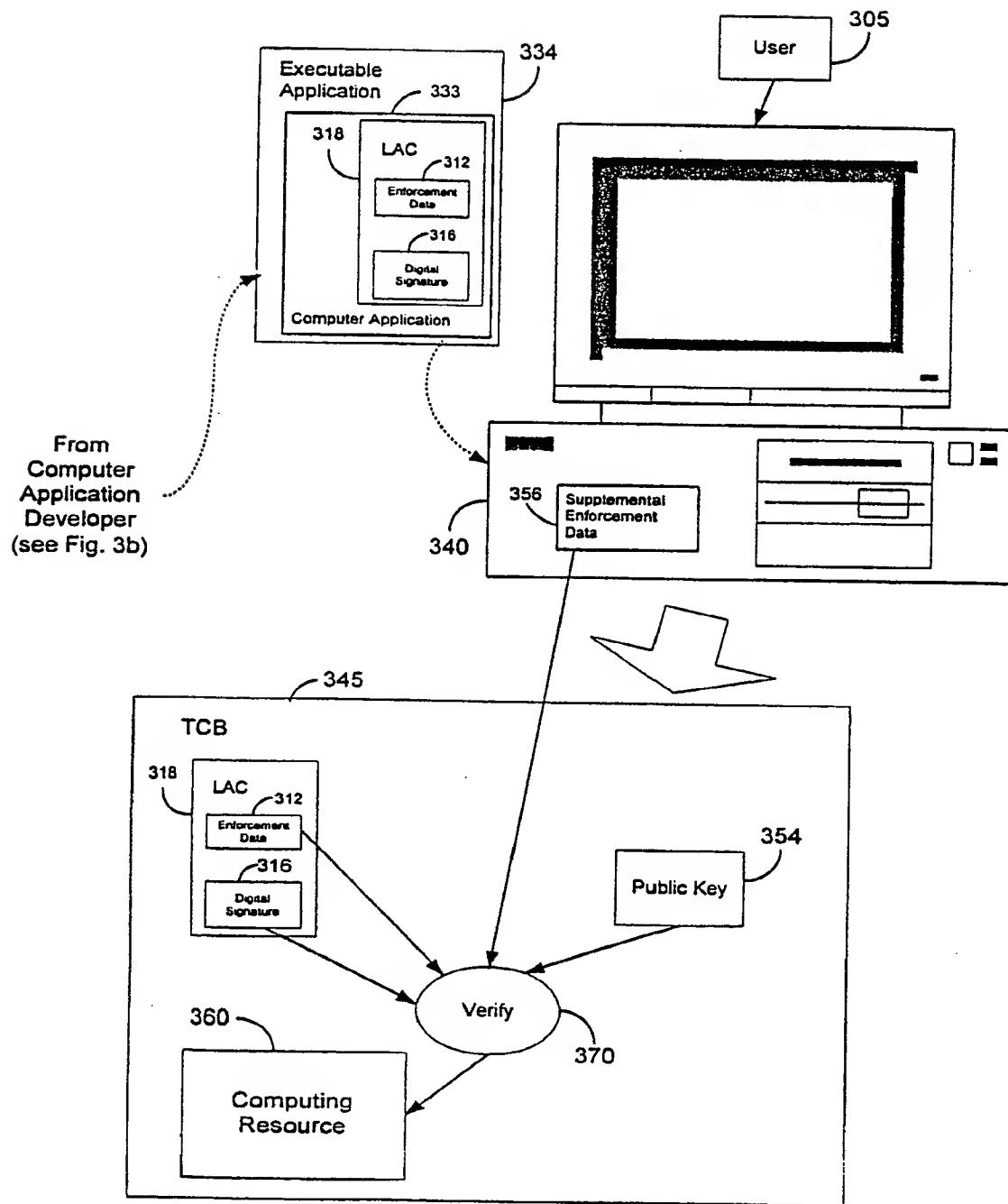


Fig. 3c

SUBSTITUTE SHEET (RULE 26)

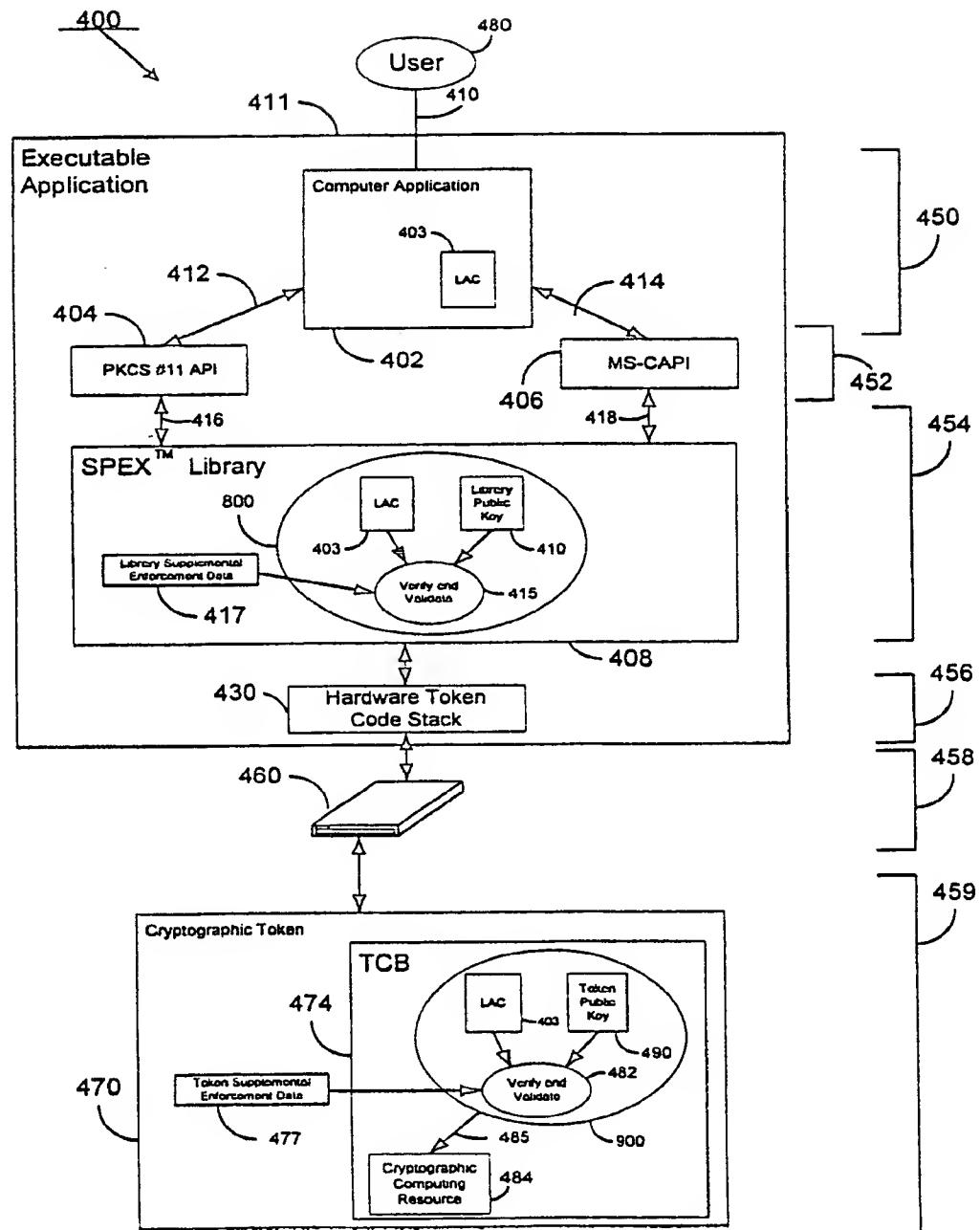


Fig. 4

SUBSTITUTE SHEET (RULE 26)

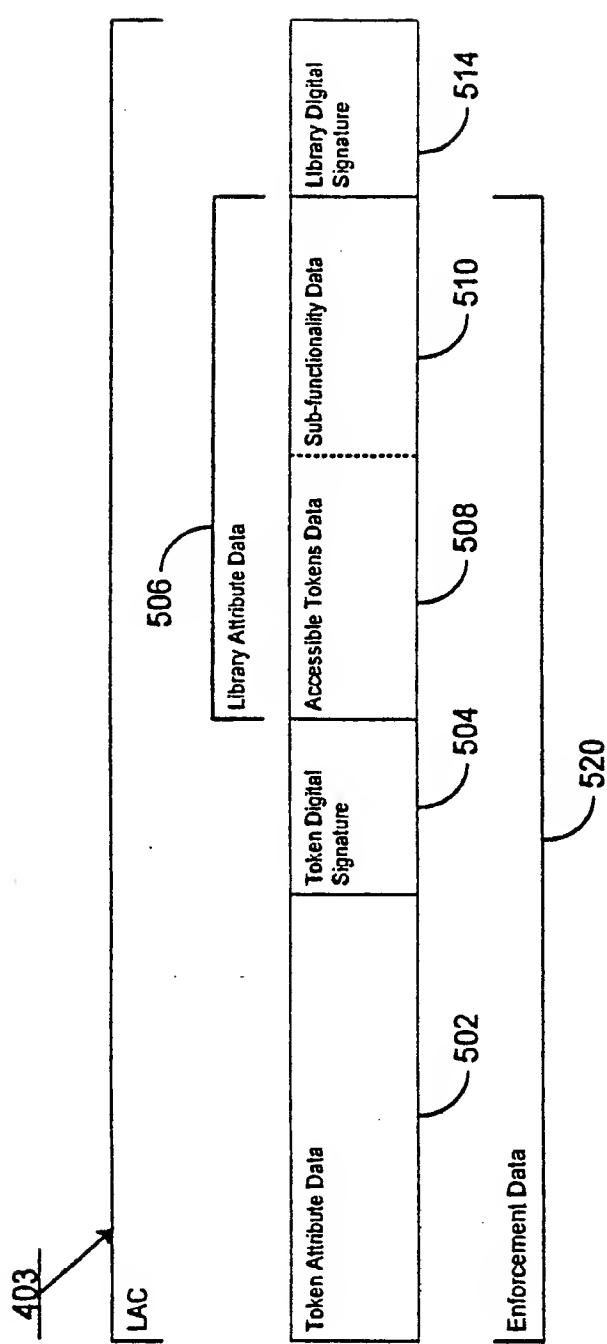


Fig. 5

SUBSTITUTE SHEET (RULE 26)

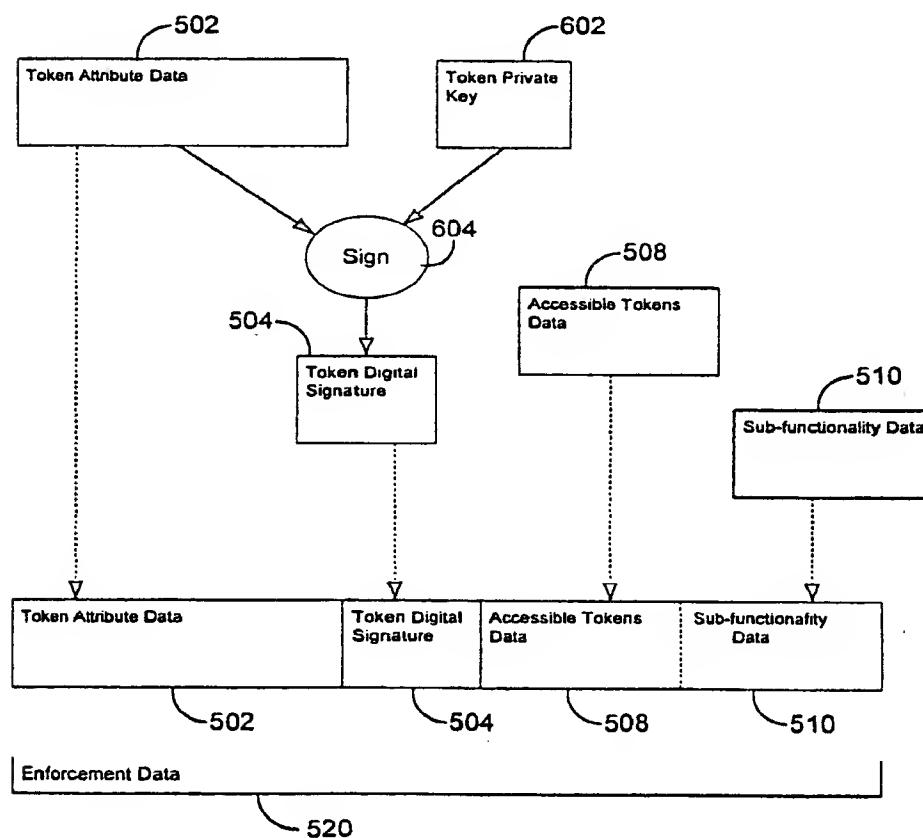


Fig. 6

SUBSTITUTE SHEET (RULE 26)

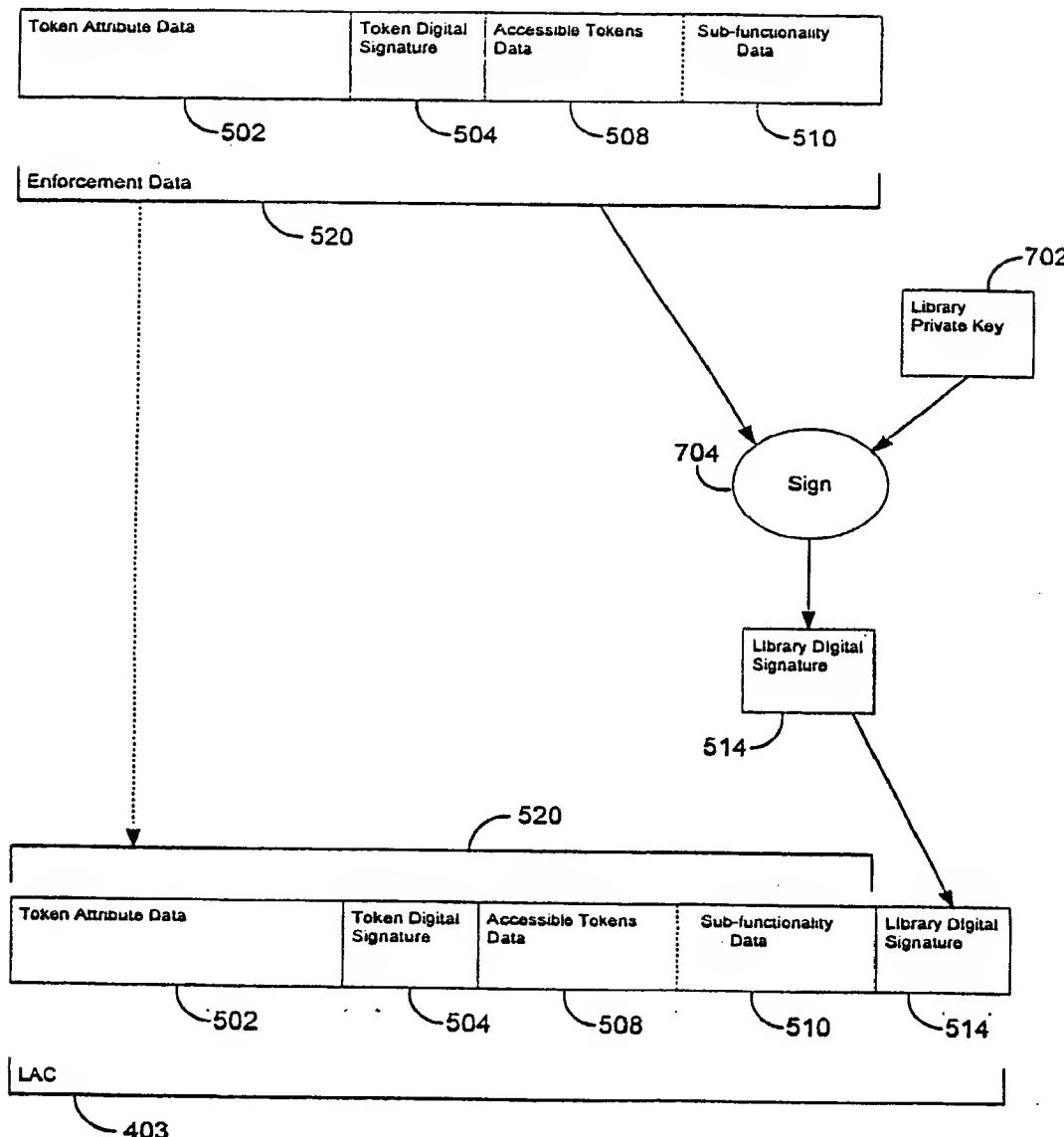


Fig. 7

SUBSTITUTE SHEET (RULE 26)

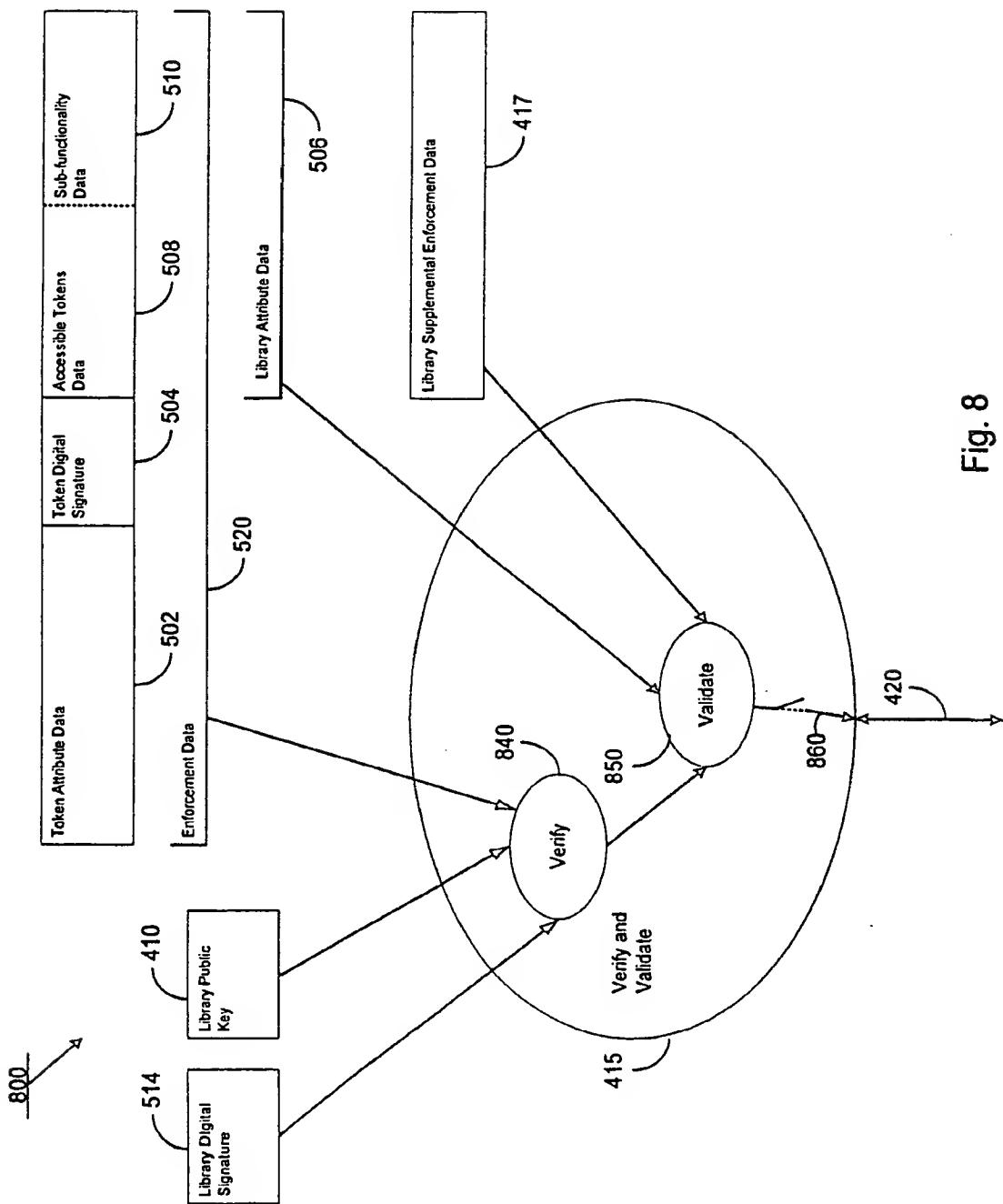


Fig. 8

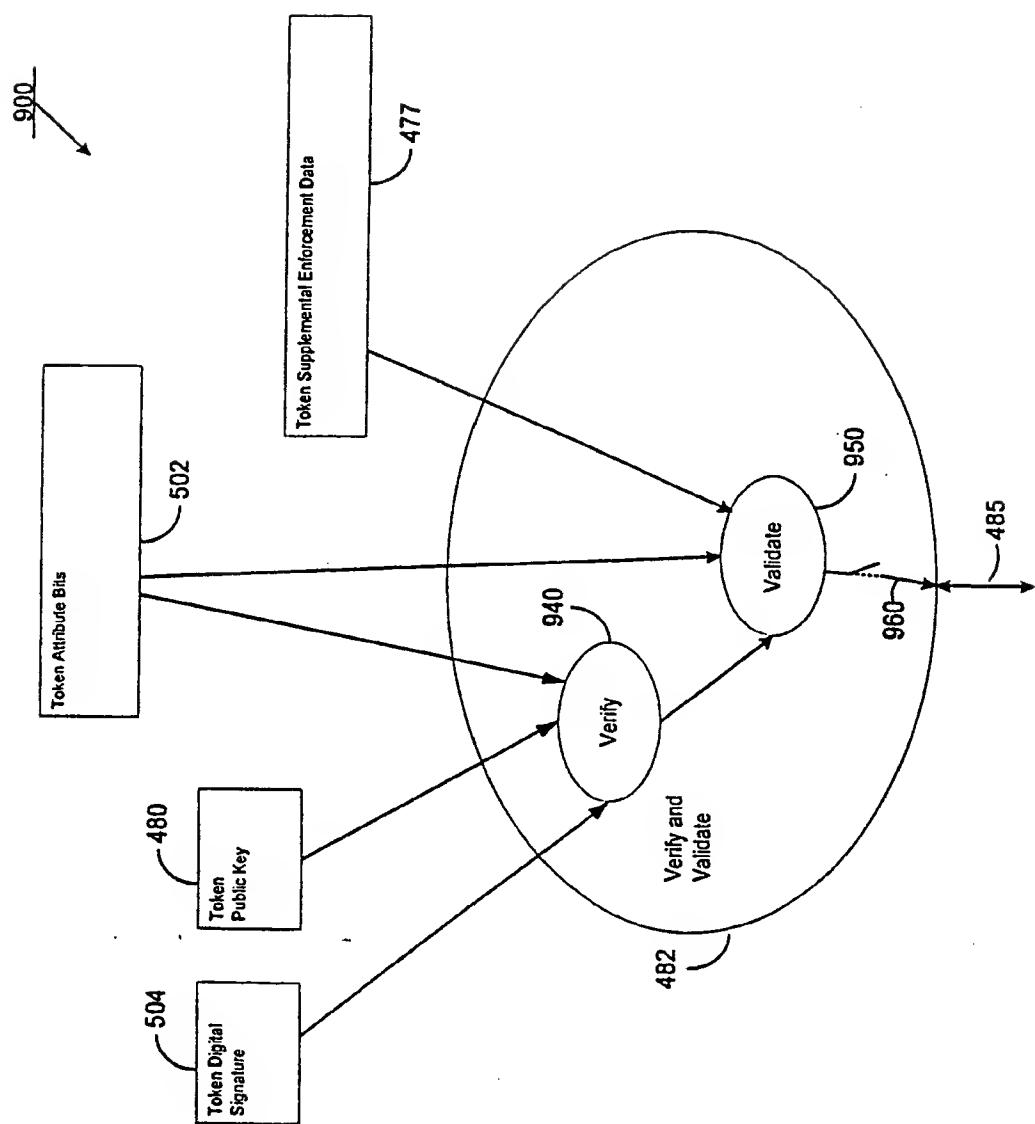


Fig. 9

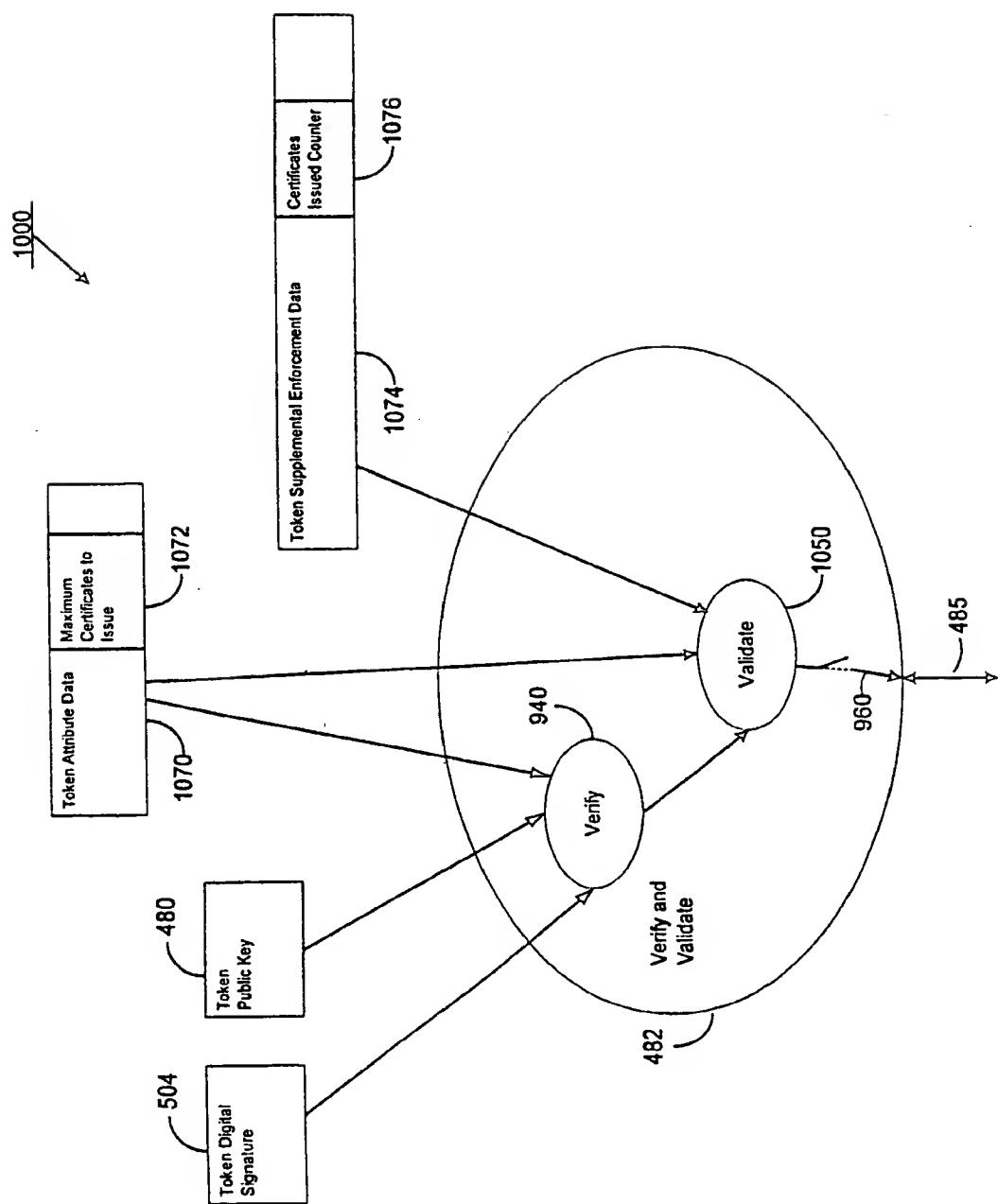


Fig. 10

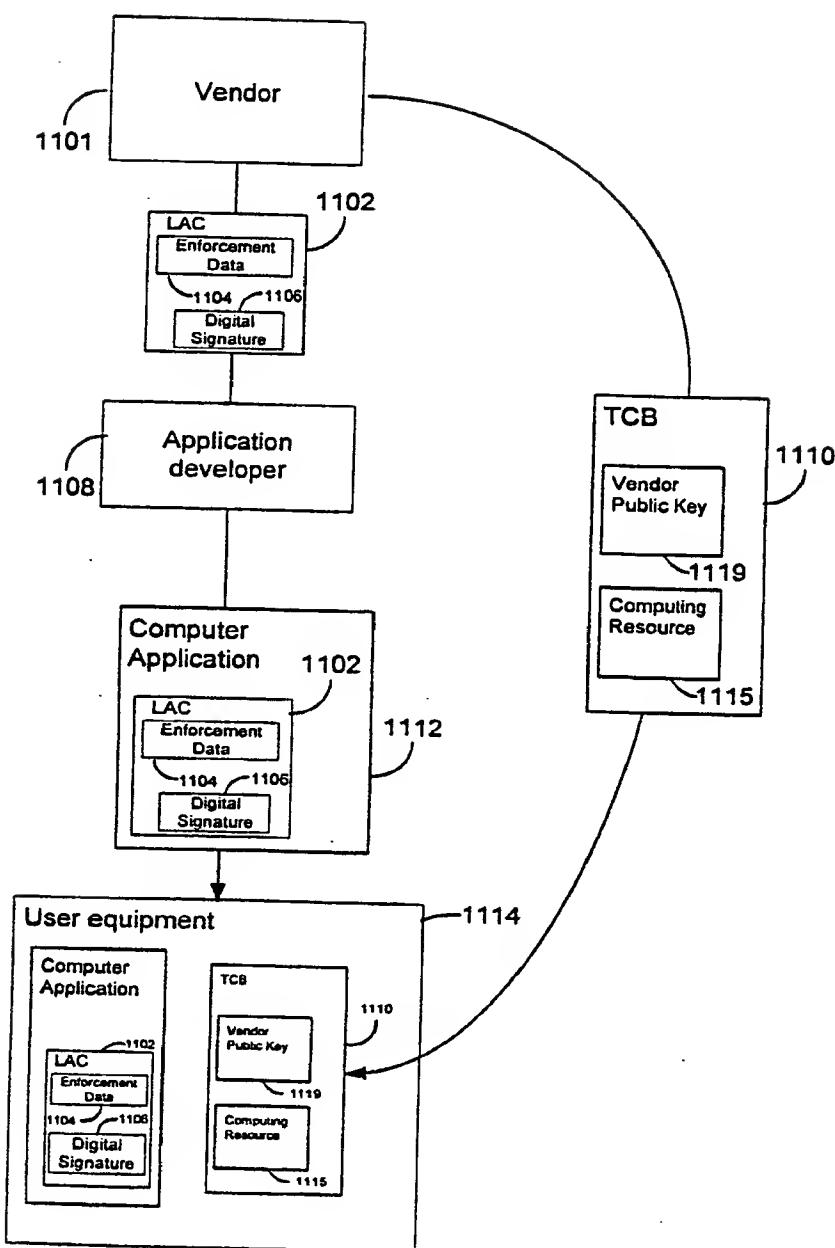


Fig. 11a

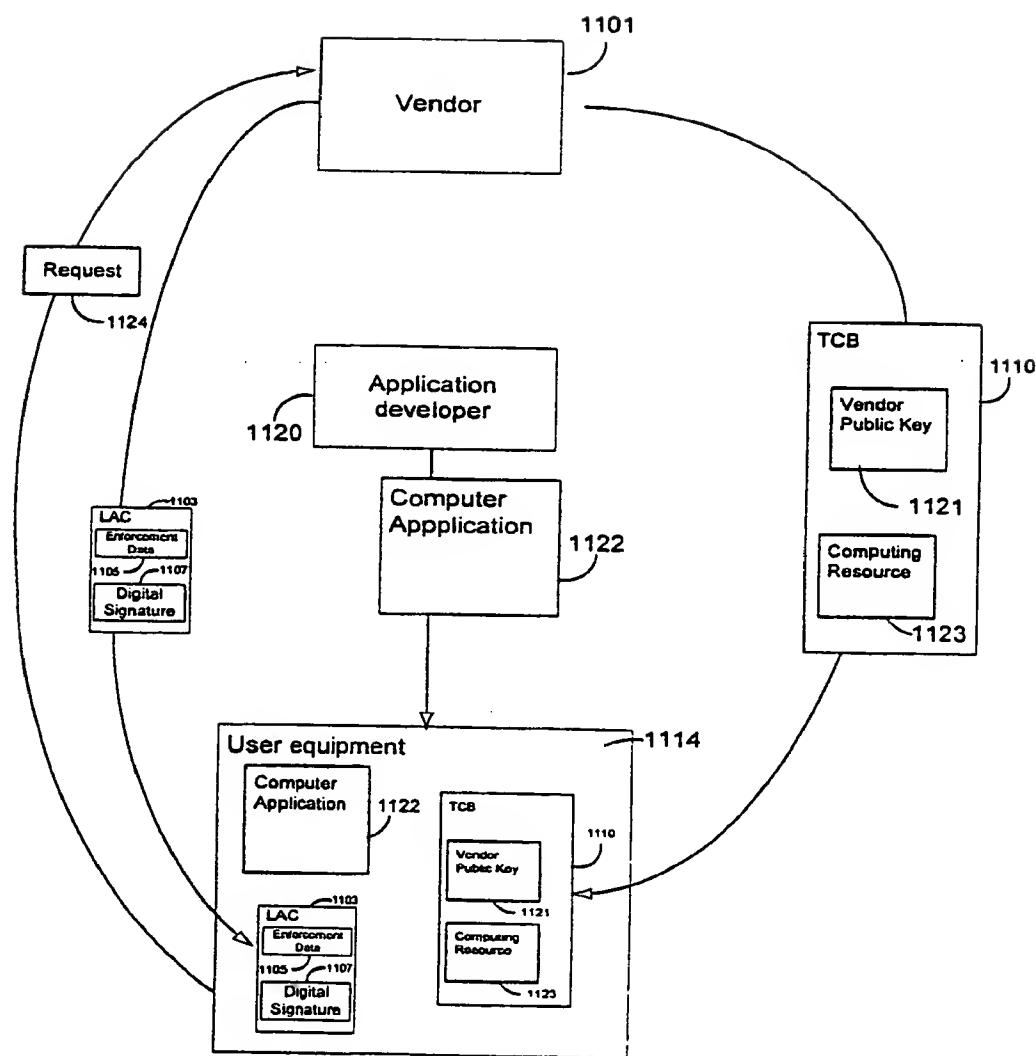


Fig. 11b

INTERNATIONAL SEARCH REPORT

Int'l Application No.

PCT/US 00/05986

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 813 132 A (IBM) 17 December 1997 (1997-12-17) abstract; figures 1,5,6 page 2, line 59 -page 3, line 39 page 4, line 26 - line 56	34,41
Y	---	35,36, 42,43
Y	WO 98 58306 A (OYLER SCOTT ;GUTHRIE JOHN (US); TECHWAVE INC (US); KRISHNAN GANAPA) 23 December 1998 (1998-12-23) abstract; figures 3,9 page 10, line 8 -page 12, line 24 page 13, line 20 -page 14, line 22 page 28, line 7 -page 31, line 3 ---	35,36, 42,43

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

18 August 2000

25/08/2000

- Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Sigolo, A

INTERNATIONAL SEARCH REPORT

Int	tional Application No
PCT/US 00/05986	

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 828 208 A (HEWLETT PACKARD CO) 11 March 1998 (1998-03-11) abstract; figures 8,9,12 column 3, line 49 -column 6, line 2 column 8, line 10 -column 12, line 9 column 15, line 13 -column 16, line 13 -----	1,22,28, 34,41
A	HOUSLEY R ET AL: "METERING: A PRE-PAY TECHNIQUE" , PROCEEDINGS OF SPIE,US,BELLINGHAM, SPIE, VOL. VOL. 3022, PAGE(S) 527-531 XP000742405 ISBN: 0-8194-2433-1 the whole document -----	28

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int'l. Application No.

PCT/US 00/05986

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP 0813132 A	17-12-1997	US 5825877 A JP 10083310 A		20-10-1998 31-03-1998
WO 9858306 A	23-12-1998	US 6073124 A AU 8150598 A		06-06-2000 04-01-1999
EP 0828208 A	11-03-1998	JP 10171648 A		26-06-1998